Solution Brief

Securing Your AWS Environments With Netskope SkopeAI

Revolutionize Security and Performance with Artificial Intelligence (AI)

Quick Glance

Organizations are currently facing several key challenges due to the usage of AI and other emerging complexities:

- Exponential Growth of Unstructured Data
- Emergence of AI-Based Threats and Evasive Social Engineering
- Proliferation of Generative AI Applications and Novel SaaS Apps
- Unpredictable User Behavior
- Unreliable Network Connectivity Performance
- Increasing Number of Newly Connected Devices

The need to address these challenges is urgent; however, most existing security solutions were not equipped to keep pace with new forms of data, the increased sophistication of threats, the unstoppable growth of SaaS apps, and the escalation of cyber warfare.

Netskope monitors traffic to and from AWS resources and applications from users located anywhere, using any device. Netskope can act in real-time to prevent movement of sensitive data, advanced threats, unauthorized users, and access to rogue accounts, exposing also suspicious activities. Netskope's Zero Trust Engine decodes activities in real-time to place activity-level restrictions on users, groups, and organizational units across more than 270 AWS services.

The Challenge

The role of artificial intelligence (AI) and machine learning (ML) in enhancing data protection and threat defense is urgent and pervasive.

In the modern cloud-enabled and hybrid work enterprise world, the rapid rise of AI has caught most organizations' cyber defenses off guard, necessitating a new approach to data security and threat protection, and emphasizing the significance of utilizing AI and ML to overcome modern cybersecurity challenges.

The Solution

SkopeAI is the Netskope suite of artificial intelligence (AI) and machine learning (ML) innovations available across the comprehensive Netskope Secure Access Service Edge (SASE) portfolio. SkopeAI solutions use AI/ML to deliver superior data protection and cyber threat defense for all sensitive data across clouds like AWS, SaaS apps, endpoints, email services and all users connecting anywhere, overcoming the limitations of conventional security technologies and delivering AI-based protection techniques not found in products from other SASE vendors. SkopeAI innovations in the Netskope unified SASE platform use AI/ML to bring data protection and threat defense techniques into the modern era with unprecedented speed and simplicity.

Deep industry expertise
AI and ML are not new to Netskope. In fact, Netskope has invested a decade delivering AI and ML solutions, and has assembled a dedicated team for AI and ML development, comprising top ML scientists, security researchers, and product engineers who possess a proven track record in solving security and fraud problems across various domains, accumulating over 100 patents, many of which are on AI/ML.

aws PARTNER Security Software Competency

SkopeAI Data Protection	AI Threat Protection	SkopeAI for Generative AI	User & Entity Behavior	SD-WAN Optimization	Device Access Intelligences
Automatically protect unstructured data with high reliability and speed with pre-trained ML classifiers Protect novel data with Train Your Own Classifiers (TYOC)	Prevent evasive attacks, polymorphic malware, new phishing, zero-day Faster detection and categorization of malware, web domains, URLs, and web content	Discover and govern the use of generative AI and novel SaaS apps Protect sensitive data across apps like Claude and coach employees in real-time	Detect users' unpredictable risky behavior Identify insiders' anomalous behavior, compromised accounts, data exfiltration	Optimal network access through enterprise-wide predictive insights WAN access anomaly detection, app performance flow analytics	Discover newly connected devices and gain deeper device context, activities and behavior Real-time detection of behavioral anomalies, threats and vulnerabilities

Challenge #1: Exponential Growth of Unstructured Data

The volume of unstructured data is growing at an alarming rate, demanding enhanced protection measures. It is estimated that nearly 80% of the projected 175 zettabytes of data by 2025 will be unstructured, including screenshots, pictures and images, web posts, and messages in collaboration apps. Organizations need more robust data detection and security mechanisms to safeguard not only their traditional structured data but also their unstructured data.

Solution #1: SkopeAI Data Protection

Main benefits:

- Detect and protect new unstructured sensitive data with high reliability and speed, including scanning Amazon S3 buckets to identify sensitive data and protect it from misuse
- Automate data protection operations and minimize human intervention

There is a pressing and unresolved challenge in data protection. Current DLP solutions are unable to adequately detect and protect a significant portion of sensitive data due to its increasingly unstructured nature. Modern data forms, such as images, screenshots, natural language, and messaging in collaboration apps and emails, embed sensitive information but are hard to analyze with conventional textual extraction and analysis tools. They also require resource-intensive processes which are difficult to scale and create DLP incident response latency. Images can be blurry, damaged, or discolored, and so indecipherable, yet still contain sensitive information.

Capabilities:

- **AI/ML Document Classification:** Netskope DLP is able to automatically recognize and classify sensitive documents into their different categories, such as source code, tax forms, patents, NDAs, and bank statements. Its ML classifiers automatically learn patterns that identify sensitive data in real time thanks to natural language processing (NLP), an AI ability to understand and derive meaning from human languages. Text content is extracted from documents and a pre-trained language model is used as an encoder to convert documents into numeric values that capture the contextual and semantic information of the documents' words. Based on these document encodings, document classifiers are trained using fully connected neural network layers. The source code classifier works differently, as it utilizes an extensive code vocabulary and common coding phrases, spanning over 20 popular programming languages, to achieve a high level of accuracy in detecting code. ML classification complements traditional text-matching and regex-based rules, ensuring high reliability and fully automated detection.

- **AI/ML Image Classification:** Netskope DLP can recognize and safeguards various sensitive data types based on its features without necessarily having to extract and read the text in them, effectively functioning like a human brain. It automatically recognizes images like source code, tax forms, patents, identification documents like passports and driver's licenses, credit and debit cards, and screenshots, etc. This technique leverages deep learning and convolutional neural networks (CNN) to accurately identify sensitive images, recognizing visual characteristics such as shapes and details to comprehend the image as a whole. AI/ML image classification works even in poor-quality images that are blurry, damaged, or discolored, yet still contain sensitive information.

- **Train Your Own Classifiers (TYOC):** Organizations also use proprietary document types and templates, personalized forms, and industry-specific files that go beyond the scope of standard ML classifiers. Netskope DLP's TYOC technology automatically identifies and categorizes new data based on a "train and forget" approach, harnessing the capabilities of AI, automation, and adaptive learning. This innovation enables organizations to confidently address their own most daunting data protection challenges while relieving policy administrators from extensive manual workloads.

These groundbreaking AI/ML-based data detection technologies greatly augment text analysis tools. It is important for DLP to be also equipped with as many text analysis tools as possible (such as thousands of data identifiers, exact data matching, document fingerprinting, optical character recognition, etc.) in symbiosis with modern AI-based engines in order to automate detection and maximize data detection accuracy. With a significantly expanded range of files today, a non-negotiable requirement is also the ability to scan thousands of different file types (png, jpg, bmp, archive formats, source code, etc.), not just the conventional documents and PDFs. Lastly, it is fundamental today to leverage rich context, empowering DLP to automatically adapt incident response to different risk scenarios.

Challenge #2: Emergence of AI-Based Threats and Evasive Social Engineering

The advent of AI has led to the emergence of new cyber threats leveraging its capabilities. Attackers can now employ AI algorithms to automate and enhance their malicious activities, including sophisticated phishing tactics that mimic harmless human behavior, making it crucial for organizations to develop advanced defense mechanisms capable of identifying and mitigating AI-based threats effectively.

Solution #2: SkopeAI Threat Protection

Main benefits:

- Prevent evasive and never-seen-before attacks, polymorphic malware, novel phishing web domains, zero-day threats, and malicious web content

- Enhance the speed of detection and categorization of malware, web domains, URLs, and web content

SkopeAI Threat Protection enhances your existing malware detection capabilities by delivering high-efficacy results and speed in detecting multivarious attacks, zero-day threats, and social engineering campaigns. SkopeAI Threat Protection leverages AI/ML for real-time, inline threat analysis and background threat analysis. For example, in real time, AI/ML defenses for malicious PE files and phishing attacks detect and block patient zero for never-before-seen threats. These SkopeAI threat defenses complement antivirus, true file type detection, IPS, and threat intelligence feeds of the latest IOCs for known threats for real-time threat protection. AI/ML threat protection defenses are also used in background analysis, sandboxing, heuristics, categorization, and to provide patient zero protection, making sure files are benign before downloading.

Capabilities

- **Deep Learning for Phishing Website Detection:** As phishing attacks are often short-lived and always changing, rendering IOCs less effective, a new approach uses generative PRT to train encoders on phishing pages. This AI/ML knowledge is then leveraged in trained decoders alongside redirect URLs to detect unknown and zero-day phishing attacks in real time within web domains. Netskope was recently awarded three patents for its phishing detection engine. With the popularity of generative AI, this new topical lure only adds to the importance of real-time phishing threat detection in web domains, plus new AI-enabled attack tools like WormGPT automating phishing attacks.
- **Detection of PE Malware Using ML Automatic Detection:** The portable executable (PE) file format is used by Windows executables, object code, and dynamic link libraries (DLLs), and is a common malware file format. The PE Classifier is an ML-based, inline, real-time defense to detect patient zero and unknown threats, and over the years has proven increasingly important as more than half of what Netskope Threat Labs detects for PE malware does not have a signature at the time of detection. In background analysis, the PE Classifier is also used in sandboxing files.
- **Web Content Dynamic URL Categorization:** Natural language processing (NLP) enables the dynamic categorization of new and uncategorized webpages with dynamic content. Using a sentence encoder and a classifier enables categorization of unknown webpages and with a high category confidence can be utilized in real time. Netskope also recommends the use of remote browser isolation (RBI) for uncategorized websites, newly registered domains, newly observed domains, and parked domains to protect users and devices.
- **Domain Generation Algorithm (DGA) Detection:** DGA domains are frequently used by modern malware attacks where protocol-level information and signatures have proven to be ineffective. SkopeAI threat protection uses a deep neural network to classify DGA domains in the background as part of Netskope web filtering.
- **Cloud Sandbox:** A cloud sandbox leverages the AI/ML defenses noted above, plus other ML models to analyze 30+ file types including behavioral analysis and the ability to defeat evasive techniques. Machine learning deep analysis with sandboxing detects unknown threats, anomalies, and behaviors. Netskope also leverages de-obfuscation and recursive file unpacking with support for 350+ families of installers, packers, and compressors, plus pre-execution analysis and heuristics for 3,500+ file format families, with 3,000+ static binary threat indicators.

Challenge #3: Proliferation of Generative AI Applications and Novel SaaS Apps

The widespread use of generative AI applications, such as ChatGPT, poses a significant risk to organizations, as it exposes them to potential data leakage and copyright violations. Measures must be taken to ensure the secure handling of sensitive information across these AI systems and other emerging shadow SaaS applications whose use is not controlled by IT.

Solution #3: SkopeAI for Generative AI

Main benefits:

- Discover and govern the responsible use of generative AI and the rapid proliferation of novel SaaS apps
- Protect sensitive data across generative AI and automatically coach employees in real time

The rise in generative AI applications exposes organizations to potential data leakage and cyber threats. It is essential to implement measures to discover, govern, and securely handle sensitive information within these AI systems and other unregulated shadow SaaS applications outside IT's control.

Capabilities

- **App Usage Visibility and Access Control:** Netskope provides the broadest visibility of SaaS apps, like generative AI, in use in the organization with ML-assisted discovery and risk categorization of new apps. Monitor employees' activities and trends with applications like Anthropic Claude and confidently control the booming use of SaaS apps (and their instances, both corporate and personal).
- **Promoting User Responsibility and Awareness:** While access to explicitly malicious apps can be filtered, security teams can give users the responsibility for accessing generative AI apps. Real-time alerts and automated coaching workflows make employees aware of the risks every time they attempt to access certain apps, and leave them the access decision after acknowledging the risks.
- **Automatic Data Protection and User Coaching:** Netskope DLP provides highly reliable detection of all sensitive data (like personally identifiable information and intellectual property), and offers several enforcement options to stop the upload and posting of sensitive data to generative AI and other SaaS apps. Real-time coaching alerts provide guidance, inform users of security policies, and minimize repeated risky behavior.
- **Data Protection Beyond Uploads:** Netskope safeguards sensitive data against unauthorized cross-application access of generative AI in the cloud. It also offers visibility into cloud-to-cloud integrations for risk assessment and mitigation.
- **Copyrights Legal Risks from AI-Generated Content:** AI-generated content poses legal risks if it infringes copyrights or other rights. Ethical concerns like fairness and accountability also arise. Netskope can analyze data that is downloaded from these apps and apply controls in real time.

While generative AI and other SaaS apps have the potential to improve work efficiency, they also expose sensitive data to external threats. As businesses continue to adopt generative AI and increase the use of SaaS apps, it is essential to prioritize data security measures to mitigate potential risks and ensure sustainable growth.

Challenge #4: Unpredictable User Behavior

Employees' behavior can be unpredictable, and their actions can often lead to data breaches. To identify suspicious activities, malicious or inadvertent, organizations today are implementing strong access controls and employing standard user behavior analytics, but the complexity of the contextual information that must be taken into account is becoming too large.

Solution #4: SkopeAI Behavioral Analytics

Main benefits:

- Detect unpredictable risky behavior of both malicious insiders and negligent insiders
- Identify anomalous behaviors for insiders, compromised accounts and devices, and data exfiltration

Malicious insider behaviors evolve rapidly, requiring a dynamic approach. A trainer machine learning model contextual information that must be taken into account is becoming too large. trained on data from the previous month may not perform optimally in the current month. To effectively detect these evolving patterns, it is essential to continuously update and retrain a machine learning model using all the contextual data available for long periods of time. By incorporating real-time data into the system, the model can adapt and maintain its effectiveness in identifying emerging threats and malicious activities.

Capabilities

- **AI/ML Behavior Anomaly Detection:** The Netskope SkopeAI user and entity behavior analytics (UEBA) uses over 50 trained models with 100+ detectors from inline and API inspection to discern normal behavior patterns from baselines and peer groups versus those that originate from malicious insiders, compromised accounts, brute-force attacks, and data exfiltration attacks. The solution logs and monitors all user activities continuously, leveraging AI/ML algorithms to identify and flag anomalous behavior. In addition to alerting administrators about these anomalies, the solution assigns a risk score to each user. This risk score is utilized as a matching criterion in zero trust data access policies. For instance, users with lower risk scores may be denied access to sensitive data in the future.
- **Ransomware Attack Detection:** The encrypted file classification ML model is designed to accurately identify whether an individual file is encrypted. To accurately detect ransomware attacks, Advanced UEBA plays a crucial role by generating user-level alerts when an anomalous amount of encrypted data movements occurs. For instance, if an infected user uploads a large number of encrypted files to a managed cloud app, this behavior stands out as highly unlikely and abnormal compared to the typical patterns exhibited by the same user, their peer groups, and other users within the organization. By leveraging these detection mechanisms, organizations can effectively identify potential ransomware attacks and take appropriate actions to mitigate the risks.

Challenge #5: Unreliable Network Connectivity Performance

Network optimization and troubleshooting of SD-WAN access anomalies require the analysis of vast amounts of data such as network activity, application use, and application performance. Only the use of AI and ML can help optimize access and performance.

Solution #5: SkopeAI Borderless SD-WAN

Main benefits:

- Enhance network access and performance with AI and ML through enterprise-wide predictive insights, WAN access anomaly detection, and application performance flow analytics

Effective network optimization must leverage vast amounts of data. Borderless SD-WAN leverages AI-driven operations to monitor the network at all levels, including user activity, branches, and clouds, enabling proactive troubleshooting and comprehensive analytics. The service generates extensive data on network activity, application usage, and performance, collecting it across the entire network, including remote users, branch offices, and cloud workloads. AI/ML helps deliver enterprise-wide predictive insights, making it easier for network engineers to ensure higher network performance while end-users gain higher productivity.

Capabilities

- **AI/ML-Driven Analytics:** Borderless SD-WAN provides valuable flow analytics on application performance across the entire network, automatically determining baselines for normal network performance and application flow statistics, which consider variations based on business hours and network activity at different branch sites and remote user locations.
- **Built-in Flight Tracker View:** The built-in flight tracker view monitors users and branches in real time, flagging end-user experience issues, Service Provider SLA violations, and providing insights into traffic flows, fault locations, policy violations, and anomalies.
- **Early Identification of Anomalies and Warning Signs:** Early identification of anomalies and warning signs reduces support tickets and resolution time, enabling customers to run large-scale networks. Additionally, AI and ML automatically rectify poor network conditions for optimal performance.
- **Automated Device Troubleshooting:** Borderless SD-WAN not only provides actionable ML-based fault insights but also offers advanced troubleshooting capabilities for devices behind branches. Its auto-discovery features identify devices accessing applications within the branch or home, enabling remote IT to use integrated IoT manager for remote troubleshooting and significantly reducing resolution time.

Challenge #6: Increasing Number of Newly Connected Devices Poses a Challenge

According to IDC, it is estimated that by 2025, approximately 80 billion devices will be connected to the internet. Modern organizations are continuously introducing new types of devices, such as IoT, which require categorization. Traditionally, this process has been manual and time-consuming.

Solution #6: SkopeAI Device Intelligence

Main benefits:

- Gain deeper insights into the device context, activities, and behavior
- Detect real-time behavioral anomalies, threats, and vulnerabilities to mitigate device-initiated risks

With the rise of cyberattacks and a majority linked to device vulnerabilities, safeguarding against unmanaged and unknown devices on the network has become a vital aspect of cybersecurity. Netskope SkopeAI Device Intelligence uses AI/ML to analyze a vast amount of parameters and contextual information from connected devices, enabling proactive device classification, risk assessment, access control, and network segmentation.

Capabilities

- **Device Fingerprinting and Classification:** Device fingerprinting and classification uncovers managed, unmanaged, and IoT devices on the network. It collects device information from multiple network interfaces, protocols, traffic flow, and application heuristics, using supervised learning for the AI models to generate dynamic device context. Machine learning algorithms and predictive models create unique models and signatures for each device, enabling automated classification, device grouping based on fingerprints, and instant identification of abnormal behavior.
- **Device Anomaly Detection:** Device anomaly detection combines device characteristics, both static (i.e., type, ownership, OS, function) and dynamic (i.e., deep fingerprinting, behavior, alerts), to identify anomalies at the device level. It provides insights and analytics on device-level risks, threats, and best practices for effective threat defense. Context-driven anomaly detection reduces false positives, detects insider threats faster, and minimizes costs and personnel requirements.
- **AI/ML-Driven Device Risk and Threat Assessment:** AI/ML-driven device risk and threat assessment assesses device risk and threats, identifying known and unknown risks by correlating context, device activities, and known vulnerabilities. The solution provides patented risk assessment and generates unique risk scores for managed, unmanaged, and transient devices. Combining threat intelligence with device context enables context-aware policies for isolating risky and vulnerable devices from the network.

To learn more, visit:
www.netskope.com/SkopeAI
www.netskope.com/products/security-service-edge

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.